Docket No. 116598-00112

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Kristof De SPIEGELER GAU: 2171

SERIAL NO: 10/780,683 EXAMINER: To be assigned

FILED: February 19, 2004

FOR: EFFICIENT COMPUTER FILE BACKUP SYSTEM AND METHOD

PRIORITY REQUEST

COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA. 22313-1450

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date of U.S. Provisional Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §119(e)**.

☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
Europe	01120041.7	20 August 2001

Certified copies of the corresponding Convention Application(s)

☒ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

(B) Application Serial No.(s)

☐ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

BLANK ROME LLP

600 NEW HAMPSHIRE AVENUE, N.W.
WASHINGTON, DC 20037
TEL (202) 944-3000
FAX (202) 572-8398

Peter S. Weissman
Registration No. 40,220

Date: March 8, 2005

Europäisches Patentamt	European Patent Office	Office européen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

01120041.7

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 01120041.7
Demande no:

Anmeldetag:
Date of filing: 20.08.01
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Dedigate N.V. e
Antwerpsesteenweg 19
9080 Lochristi
BELGIQUE

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Method for deciding whether a computer file should be backed up and for restoring a previously backed up computer file

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

G06F17/00

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR

Method for deciding whether a computer file should be backed up and method for restoring a previously backed up computer file

Qualities & Benefits

1. to provide a backup solution consuming minimal bandwidth
2. to provide a backup solution consuming minimal storage
3. to provide a fully scalable & reliable backup environment
4. to provide a simple to use and fully integrated backup system

Primary Features

1. distributed login and central authentication
2. target system (server) will be backed up as scheduled using minimal storage & bandwidth
4. target system (server) can be restored to any previous backup
5. backup scheduling
6. backups can be restored to any server, connected to the same central storage server

Secondary Features

1. web user interface
2. integration with DCOS (DataCenter Technologies' Operating System)

Method

A1. Method of using a hashing key of file content for backup.
First step in the process is scanning the file system on the target machine (computer system to be backed up) and creating a hashing key – in either 32 or 64 byte modes – as a unique digital code for each of the files to be backed up. These hashing keys are stored in a local database -a database on the target machine- for further comparison.

A2. The stored hashing keys are checked against previous entries in the local database. This hashing key is used to check if a local file was ever backed up before on the target system. The hashing keys not found in the database are used in the next step of the process.

A3. The hashing keys, which are the result of step A2, are now checked against the files stored on the central storage server. The hashing keys are used only in this 3nd phase to determine if this file is already present on the central storage server. The file may be present as the result of a backup from any other server. The principle is to store a single copy of each unique file within the data center.

A4. Dispatching process of using hashing keys for backup.
Based on the hashing key the central backup server software (in front of the data repository and called DC-Protect server) will decide to which location the file needs to be dispatched. The content key is used for dispatching files to different locations in the storage network.

The method of the invention uses hashing keys to make the process of backing up data center environments automated and intelligent, resulting in bandwidth savings and minimal storage needs.

Background

History of the technology & Deficiency in prior technology

Data Centers usually comprise several computer systems, such as Internet servers. They have scalability problems using traditional backup systems. The required bandwidth and storage is not sufficient to do massive data center backup of Internet infrastructure environments.

Objective

The primary objective of the invention is to provide a better and more effective data center backup solution.
The main advantage of the invention is the minimal consumption of bandwidth and storage compared to traditional backup systems.

Drawings

Flowchart DC-Protect

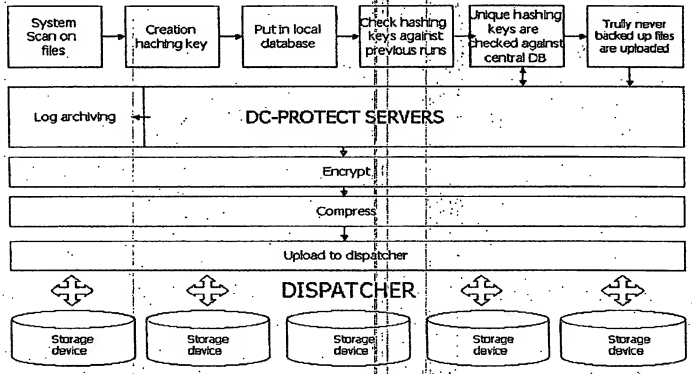

Figure "Flowchart of DC-Protect is a visual overview of the backup system and its processes".

Field of Invention

This invention relates to backup technology, and more particularly to create a solution for massive server backup in Internet data center and enterprise data center environments, resulting into a solution for disaster recovery and data protection.

Detailed Description

1. Traditionally, backup solutions hugely increase network traffic and use enormous storage capacity by doing incremental or full backups of servers.

2. The invention uses content hashing keys to make intelligent decision to backup certain data or not.
3. New is the process of using a hashing mechanism to check if a file is unique in a backup solution. Unique and not yet backed up files will be stored on a central storage system. The new method matches newly created content keys against all previously generated content keys to make a backup decision, all resulting in a holistic approach of doing backup.
4. The new method has a minimal consumption of bandwidth and a minimal use of storage capacity.

How does it work
Backup agents scans all computer files on target system (computer system, for example a server) and creates a hashing key for each of the selected files.
List of content keys is compared locally to the previously generated content keys (from previous backup).
New content keys are checked against the central backup system to see if the file is already backed up originating from another server.
If file is really unique then and only then the file will be secured and transferred to our backup system (central storage server).

To restore a unique file, the target server requests the hashing key for that file from the local database (on the target server) and retrieves that file from the central storage server.

Claims

1. Method for deciding whether a computer file should be backed up, comprising:

computing a hashing key from at least a portion of the content of said file,

verifying if said hashing key is already present in a database,

deciding to back up said file only if said hashing key is not present in the database.

2. Method according to claim 1, wherein said database is stored in the same computer system as said computer file, and wherein said file is backed up in a different central storage server.

3. Method according to claim 2, further comprising a step of checking said hashing key against files already backed up in said central storage server, and deciding to back up said file only if said hashing key does not correspond to any file in said central storage server.

4. Method according to claim 3, wherein said file is renamed to its hashing key once stored in said backup server.

5. Method according to one of the preceding claims, wherein a plurality of computer systems are connected with said central storage server, and wherein said computer file is not backed up if it is already present as the result of a backup from another computer file.

6. Method according to the preceding claim, wherein the location of said backed up file in said central storage server depends on said hashing key.

7. Method according to the preceding claim, wherein said central storage server comprises a plurality of storage devices.

8. Method for restoring a previously backed up computer file, comprising:

requesting the hashing key corresponding to said computer file from a database storing a previously computed hashing key for each backed up computer file,

using said hashing key to retrieve said backed up computer file.

9. Method according to claim 8, wherein the location at which said computer file has been backed up depends on said hashing key.

10. Method according to claim 9, wherein the name under which said computer file has been backed up depends on said hashing key.

11. Computer program product stored on a computer usable medium and comprising computer readable program means for causing said computer to perform the steps of one of the preceding claims.

12. Computer system comprising an area portion in which a database is stored comprising a hashing key for all previously backed up files.